

**【CLAIMS】****【Claim 1】**

In a key exchange method for mutual authentication at a subscriber station accessed to an authentication server through a wired/wireless communication, a two-factor authenticated key exchange method comprising:  
5

(a) the subscriber station transmitting a key to the authentication server, the key being generated using an identifier of the subscriber station and a public key of the authentication server;

(b) the subscriber station receiving a random number generated by the authentication server;  
10

(c) using the received random number, a password predefined in the subscriber station, and a key stored in a token, and transmitting an encrypted first specific value and a generated authenticator of the subscriber to the authentication server;

(d) the subscriber station receiving an authenticator of the authentication server according to an authentication success on the transmitted authenticator of the subscriber by the authentication server; and  
15

(e) the subscriber station using the secret key and the password, authenticating the received authenticator of the authentication server, and receiving the authenticator of the authentication server when the authentication is successful.  
20

**【Claim 2】**

The two-factor authenticated key exchange method of claim 1, wherein the key stored in the token is a symmetric key.

**【Claim 3】**

The two-factor authenticated key exchange method of claim 1, further comprising: before (a),

the subscriber station determining the symmetric key and the password used for a symmetric key algorithm and sharing the symmetric key and the password with the authentication server during a registration process; and

the subscriber station generating a random number and precomputing the first determined value when the subscriber station does not exchange a key for authentication with the authentication server.

**【Claim 4】**

The two-factor authenticated key exchange method of claim 1 or 3, wherein the subscriber station stores the password and the public key of the authentication server in the token.

**【Claim 5】**

The two-factor authenticated key exchange method of claim 1 or 3, wherein the generated key is generated by applying a one-way Hash function to an identifier of the subscriber station and the public key of the authentication server in (a).

**【Claim 6】**

The two-factor authenticated key exchange method of claim 1 or 3,

wherein (c) comprises:

applying the Hash function to the received random number, the password, and the key stored in the token, and generating a second predetermined value;

5 using the second predetermined value and encrypting the first predetermined value;

using the random number and the first predetermined value, and generating the subscriber's session key;

10 applying the Hash function to the generated session key, the password, the key stored in the token, and the identifier of the subscriber station, and generating the subscriber's authenticator; and

transmitting the encrypted first predetermined value and the subscriber's authenticator to the authentication server.

**【Claim 7】**

15 The two-factor authenticated key exchange method of claim 6, wherein (e) comprises:

applying the Hash function to the subscriber's session key, the password, the key stored in the token, and the public key of the authentication server, and generating a third predetermined value;

20 determining whether the generated third predetermined value corresponds to the authenticator of the authentication server received from the authentication server; and

determining that the authentication between the subscriber station and the authentication server is successful and receiving the authenticator of the authentication server when the generated third predetermined value is found to correspond to the authenticator of the authentication server.

5      **【Claim 8】**

In a method for an authentication server accessed to a subscriber station for wired/wireless communication to exchange a key for mutual authentication, a two-factor authenticated key exchange method comprising:

10      (a) the authentication server receiving a key which is generated by the subscriber station by using an identifier and a public key of the authentication server;

15      (b) the authentication server using the value received from the subscriber station, detecting the subscriber's password, the key stored in a token, and a public key of the authentication server, generating a random number, and transmitting the random number to the subscriber station;

(c) the authentication server receiving an encrypted value generated by the subscriber station and the subscriber's authenticator based on the transmitted random number;

20      (d) the authentication server establishing a first predetermined value generated by using the password, the key stored in the token, and the random number to be a secret key, decrypting the encrypted value received in (c) to generate a second predetermined value, authenticating the received

authenticator of the subscriber based on the second predetermined value, and receiving the subscriber's authenticator when the authentication is successful; and

(e) the authentication server using the password, the key stored in the token, and the public key, and transmitting the authenticator of the authentication server to the subscriber station.

**【Claim 9】**

The two-factor authenticated key exchange method of claim 8, wherein the key stored in the token is a symmetric key.

**10      【Claim 10】**

The two-factor authenticated key exchange method of claim 9, further comprising: before (a), the authentication server determining the symmetric key and the password used for a symmetric key cryptosystem and sharing the symmetric key and the password with the subscriber station during a registration process.

**15      【Claim 11】**

The two-factor authenticated key exchange method of claim 8 or 10, wherein the authentication server stores the key stored in the token, the password, and the secret key of the authentication server in a security file database.

**20      【Claim 12】**

The two-factor authenticated key exchange method of claim 8 or 10,

wherein (d) comprises:

applying the Hash function to the password, the key stored in the token, and the random number, and generating the first predetermined value;

establishing the generated first predetermined value to be a secret key,  
5 decrypting the received encrypted value, and generating the second predetermined value;

using the generated second predetermined value, the public key of the authentication server, and the random number, and generating a session key of the authentication server;

10 determining whether the value obtained by applying the Hash function to the generated session key, the password, the key stored in the token, and an identifier of the subscriber station corresponds to the received authenticator of the subscriber; and

determining that the authentication for the subscriber is found to be  
15 successful and receiving the authenticator of the subscriber when the value corresponds to the received authenticator of the subscriber.

**【Claim 13】**

The two-factor authenticated key exchange method of claim 12, wherein the session key of the authentication server is used to generate the  
20 authenticator of the authentication server in (e).

**【Claim 14】**

The two-factor authenticated key exchange method of claim 1 or 8,

wherein the subscriber station transmits a user name, a hashed value of the public key of the authentication server, and a domain name to the authentication server when the identifier of the subscriber station uses the NAI (network access ID) format in order to support global roaming and billing in (a).

5       **【Claim 15】**

In a mutual authentication method through a two-factor authenticated key exchange between a subscriber station and an authentication server in a wireless communication system in which the subscriber station and the authentication server are accessed through an access point, an authentication  
10       method through a two-factor authenticated key exchange comprising:

(a) the subscriber station receiving an identifier request from the access point;

(b) the subscriber station transmitting a key which is generated by using an identifier of the subscriber station and a public key of the authentication  
15       server to the authentication server through the access point;

(c) the authentication server using the key received from the subscriber station, detecting the subscriber's password, the secret key, and the public key of the authentication server, generating a random number, and transmitting the random number to the subscriber station through the access point;

20       (d) the subscriber station using the received random number, the password, and the key stored in the token, and transmitting an encrypted first predetermined value and the generated authenticator of the subscriber to the

authentication server through the access point;

(e) the authentication server establishing a second predetermined value generated by using the password, the key stored in the token, and the random number to be a secret key, decrypting the encrypted value received in (d),  
5 authenticating the received authenticator of the subscriber based on the decrypted value, and when the authentication is found successful, transmitting an authenticator of the authentication server generated by using the password, the key stored in the token, and the public key to the subscriber station through the access point;

10 (f) the subscriber station using the key stored in the token and the password, authenticating the received authenticator of the authentication server, and transmitting an authentication result to the authentication server through the access point; and

(g) the authentication server transmitting an access permission for the  
15 subscriber to the subscriber station through the access point when the authentication result transmitted from the subscriber station is found successful.

**【Claim 16】**

The authentication method of claim 15, wherein the key stored in the token is a symmetric key.

20 **【Claim 17】**

The authentication method of claim 15 or 16, wherein an extensible authentication protocol is used between the subscriber station and the access



point, and

a RADIUS protocol is used between the access point and the authentication server.

**【Claim 18】**

5           In a method for exchanging keys for mutual authentication at a subscriber station accessed to an authentication server through a wired/wireless communication, a recording medium storing a program comprising:

          (a) the subscriber station transmitting a key generated by using the identifier of the subscriber station and the public key of the authentication server  
10       to the authentication server;

          (b) the subscriber station receiving a random number generated by the authentication server;

          (c) the subscriber station using the received random number, the password predefined at the subscriber station, and the key stored in the token,  
15       and transmitting an encrypted first predetermined value and the generated authenticator of the subscriber to the authentication server;

          (d) the subscriber station receiving the authentication server's authenticator generated by the authentication server according to the successful authentication on the transmitted authenticator of the subscriber by the  
20       authentication server; and

          (e) the subscriber station using the key stored in the token and the password, authenticating the received authenticator of the authentication server,

and receiving the authenticator of the authentication server when the authentication is successful.

**【Claim 19】**

The recording medium of claim 18, wherein the key stored in the token is  
5 a symmetric key.

**【Claim 20】**

In a method for exchanging keys for mutual authentication at an authentication server accessed to a subscriber station through a wired/wireless communication, a recording medium storing a program comprising:

10 (a) the authentication server receiving a value which is generated by using an identifier and a public key of the authentication server by the subscriber station;

(b) the authentication server using the value received from the subscriber station, detecting the user's password, a key stored in a token, and a  
15 public key of the authentication server, generating a random number, and transmitting the random number to the subscriber station;

(c) the authentication server receiving the encrypted value generated by the subscriber station and an authenticator of the subscriber based on the transmitted random number;

20 (d) the authentication server establishing a first predetermined value which is generated by using the password, the key stored in the token, and the random number to be a secret key, decrypting an encrypted value received in

(c) to generate a second predetermined value, authenticating the received authenticator of the subscriber based on the generated second predetermined value, and receiving the authenticator of the subscriber when the authentication is found successful; and

5           (e) the authentication server transmitting the authenticator of the authentication server generated by using the password, the key stored in the token, and the public key to the subscriber station.

**【Claim 21】**

10           The recording medium of claim 20, wherein the key stored in the token is a symmetric key.